UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/755,450	01/13/2004	Igor Garrievich Muttik	03.047.01	1086

7590 07/17/2008

Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172-1120

EXAMINER	
LANIER, BENJAMIN E	
ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
07/17/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/755,450	MUTTIK, IGOR GARRIEVICH	
	Examiner	Art Unit	
	BENJAMIN E. LANIER	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 April 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-54* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-54* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 28 April 2008 has been entered.

Response to Amendment

2. Applicant's amendment filed 28 April 2008 amends claims 1, 18, 35. Claims 2, 14, 19, 31, 36, and 48 have been cancelled. Claim 54 has been added.

Response to Arguments

3. Applicant argues, "applicant clearly claims 'modifying said set of rules **such that** at least one secondary set of one or more external program calls are more strongly associated with malicious computer program activity' (see this or similar, but not necessarily identical language in the independent claims-emphasis added), as claimed. Therefore, it is clear that applicant's claimed 'said at least one secondary set of one or more external program calls are more strongly associated with malicious computer program activity' (emphasis added), as claimed is definite." This argument is not persuasive because Applicant has failed to provide any actual rationale as to why the claims are definite. Additionally, it is unclear how modifying "said set of rules" has any effect on a set of program calls that has already been logged.

4. Applicant argues, "only generally disclosing that '[t]he behavior pattern is preferably used to analyze the behavior of the unknown program,' as in van der Made, does not specifically

meet a 'secondary set of identifying code operable to identify, within said stream, at least one secondary set of one or more external program calls associated with said primary set of one or more external program calls' (emphasis added), particularly where the 'primary set of one or more external program calls match[es] one or more rules indicative of malicious computer program activity from among a set of rules' (emphasis added), in the context claimed by applicant." This argument is not persuasive because van der Made discloses multiple behavior patterns, where an earlier behavior pattern would be equivalent to the secondary set of programs calls, and a later behavior pattern indicative of a virus infection would be equivalent to the primary set of program calls.

5. Applicant argues, "Simply nowhere in the excerpts relied on by the Examiner is there any teaching or suggestion of a 'secondary set of one or more external program calls associated with said primary set of one or more external program calls,' as claimed." This argument is not persuasive because van der Made specifically discloses that "generated behavior pattern does not change significantly between version updates, but does change dramatically when a virus infects a program." See column 6, lines 30-32. van der Made meets the limitation in question because any one of the behavior patterns logged by the virtual machine that is not considered "drastically" changed can be considered the claimed "secondary set of one or more external program calls," while the "drastically" changed behavior pattern would be considered the "primary set". These patterns are associated to the extent that they are behavior patterns of the same program.

6. Applicant argues, "in van der Made, clearly fail to teach 'modifying code operable to modify said set of rules such that said at least one secondary set of one or more external program

calls are more strongly associated with malicious computer program activity,' (emphasis added), as claimed by applicant." This argument is not persuasive because van der Made shows (Col. 11, lines 36-60) that the rules used to detect virus behaviors are changed from when an analysis showed to virus pattern, to a later analysis that did shows a virus pattern.

7. Applicant's argument that van der Made does not disclose the limitations of claim 2, which have now been amended into independent claim 1, is not persuasive. In van der Made, the behavior pattern that did not show a virus pattern would precede the behavior pattern that "drastically" changed after infection.

8. Applicant's argument with respect to the claim language of claim 14, now amended into independent claim 1, is not persuasive because van der Made shows (Col. 11, lines 36-60) that the rules used to detect virus behaviors are changed from when an analysis showed to virus pattern, to a later analysis that did shows a virus pattern.

9. Applicant argues, "van der Made, clearly do not teach that a 'set of rules is subject to a validity check after modification to determine if said set of rules is more effectively detecting malicious computer activity' (emphasis added), as claimed by applicant." This argument is not persuasive because van der Made effectively shows that changed behavior analysis detected 4% of the virus that the initial analysis did not detect, and therefore meets the claim limitation.

10. Examiner believes that the remaining arguments are fully addressed in light of the above remarks.

Specification

11. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the

following is required: The phrase "computer readable medium," is not found to have proper antecedent basis in the specification, however it is necessary to use this terminology in order to properly define the claim within the boundaries of statutory subject matter, because the phrase "computer readable medium," appears to only reasonably convey hardware storage and forms of portable, physical article media to one of ordinary skill in the art. In order to overcome the objection, an amendment to the specification is necessary constituting a non-exhaustive statement of what the phrase "computer readable medium" would be as it would have been known to one of ordinary skill in the art at the time of the invention, in order to verify that the term "computer readable medium," could not be taken in the context of non-statutory subject matter.

Claim Rejections - 35 USC § 112

12. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

13. Claims 1, 3-18, 20-35, 37-47, 49-54 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

14. The term "more strongly associated" in claims 1, 18, and 35 is a relative term which renders the claims indefinite. The term "more strongly associated" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

15. Additionally, it is unclear how modifying "said set of rules" has any effect on a set of program calls that has already been logged.

Claim Rejections - 35 USC § 102

16. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

17. Claims 1, 8-10, 13, 17, 18, 25-27, 30, 34, 35, 42-44, 47, and 51-54 rejected under 35 U.S.C. 102(e) as being anticipated by van der Made (Made), U.S. Patent No. 7,093,239.

As per claims 1, 2, 18, 17, 35 and 36:

Made discloses a computer program product operable to detect malicious computer program activity, comprising:

logging code operable to log a stream of external program calls (10:18-29);

primary set identifying code operable to identify, within said stream of external program calls, a primary set of one or more external program calls matching one or more rules indicative of malicious computer program activity from among a set of rules;

secondary set identifying code operable to identify, within said stream, at least one secondary set of one or more external program calls associated with said primary set of one or more external program calls; and

modifying code operable to modify said set of rules such that said at least one secondary set of one or more external program calls are more strongly associated with malicious computer program activity (6:12-24 and 11:46-60)

wherein one of said at least one secondary set of one or more external program calls precedes said primary set of one or more external program calls within said stream of external program calls (6:12-24).

Made discloses a computer program product wherein said set of rules is modified to include a new rule corresponding to said secondary set of one or more external program calls, said new rule thereafter being used in addition to other rules within said set of rules (11:46-59).

As per claims 8-10, 25-27 and 42-22:

Made discloses a computer program product wherein said set of rules include at least one of: one or more pattern matching rules; and one or more regular expression rules, wherein said set of rules are responsive to ordering of external program calls and said modifying code dynamically adapts said set of rules in response to detected streams of external program calls performing malicious computer program activity (5:16-39).

As per claims 13, 30 and 47:

Made discloses a computer program product wherein said stream of external program calls are logged following emulation of execution of a computer program (5:16-39).

As per claims 17, 34 and 51:

Made discloses a computer program product wherein said set of rules is subject to a validity check after modification to determine if said set of rules is more effectively detecting malicious computer program activity (12:26-41).

As per claims 52-53:

Made discloses a computer program product further comprising applying high level rules to the modified set of rules, and promoting said modified set of rules from a temporary set to a permanent set based on the application of the high level rules to the modified set of rules and on the determination that the modified set of rules decreased malicious traffic (10:18-11:23, 12:26-41).

As per claim 54:

Made discloses promoting code operable to determine whether said modified set of rules slows malware propagation, and to promote said modified set of rules from a temporary set to a permanent set if it is determined that said modified set of rules slows said malware propagation (Col. 12, lines 26-41).

Claim Rejections - 35 USC § 103

18. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

19. Claims 3-5, 20-22 and 37-39 rejected under 35 U.S.C. 103(a) as being unpatentable over Made, U.S. Patent No. 7,093,239 as applied to claims 1, 18 and 35 above and further in view of Khazan et al. (Khazan), U.S. PG-PUB 2005/0108562.

As per claims 3, 20 and 37:

Khazan substantially teaches a computer program product wherein said external program calls are application program interface calls to an operating system (paragraph 0042).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to utilize the invention of Khazan in combination with the invention of Made because executing the malicious code detector of Khazan in a simulation mode would allow the executables being tested to display the malicious code symptoms without actually hurting the computer system it resides on as taught by Khazan (paragraph 0111).

As per claims 4, 5, 21, 22, 38 and 39:

Khazan substantially teaches a computer program product wherein each of said external program calls has one or more characteristics compared against said set of rules, wherein said

one or more characteristics include: a call name; a return address; one or more parameter values; and one or more returned results (paragraph 0042).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to utilize the invention of Khazan in combination with the invention of Made because executing the malicious code detector of Khazan in a simulation mode would allow the executables being tested to display the malicious code symptoms without actually hurting the computer system it resides on as taught by Khazan (paragraph 0111).

20. Claims 6-7, 23-24 and 40-41 rejected under 35 U.S.C. 103(a) as being unpatentable over Made as applied to claims 1, 18 and 35 above, and further in view of Obrecth et al. (Obrecht), U.S. PG-PUB 2004/0064736.

As per claims 6-7, 23-24 and 40-41:

Obrecht substantially teaches a computer program product wherein rules within said set of rules specify score values of external program calls having predetermined characteristics and a set of one or more external program calls is identified as corresponding to malicious computer program activity if said set of one or more external program calls has a combined score value exceeding a threshold level and the score level associated with the secondary set is increased to more strongly associate the secondary set with malicious program activity (paragraph 0039).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to utilize the score and weight system of Obrecht with the emulation system of Made in order to create a more robust computer system as taught by Obrecht (paragraph 0056).

21. Claims 11-12, 28-29 and 45-46 rejected under 35 U.S.C. 103(a) as being unpatentable over Made as applied to claim 1, 18 and 35 above, and further in view of Judge, U.S. Patent No. 7,096,498.

As per claims 11-12, 28-29 and 45-46:

Judge substantially teaches a computer program product wherein at least changes within said set of rules are transmitted to one or more remote computer such that said one or more remote computers can use said modified set of rules without having to suffer said malicious computer program activity (abstract) and to a rules supplier (20:5-34).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to propagate the rules to other systems in order to get a global view of traffic patterns as disclosed in Judge (6:58-7:10).

Conclusion

22. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Swiler, U.S. Patent No. 7,013,395

Yoshida, U.S. Patent No. 7,337,155

Ko, U.S. Publication No. 2002/0138755

Eskin, U.S. Patent No. 7,162,741

Warrender, "Detecting Intrusions Using System Calls: Alternative Data Models", 1999.

Hofmeyr, "Intrusion Detection using Sequences of System Calls", 1998.

23. Any inquiry concerning this communication or earlier communications from the examiner should be directed to BENJAMIN E. LANIER whose telephone number is (571)272-3805. The examiner can normally be reached on M-Th 6:00am-4:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Benjamin E Lanier/
Primary Examiner, Art Unit 2132